TEESSIDE UNIVERSITY

AND

MANAGEMENT DEVELOPMENT INSTITUTE OF SINGAPORE

Course (Batch)	: Bachelor of Science (Honours) Cybersecurity and Networks (BNSE22304A, BNSE22305A)
Module Code and Title	: CIS2026-N Ethical Hacking
MDIS Module Tutor	: Mr Ku Chee Chiang, William
Assessment	: Individual Report
Due Date	: 1 September 2023
Module Weightage	: 100%

TEESSIDE UNIVERSITY

IN-COURSE ASSESSMENT (ICA) SPECIFICATION

Module Title: Ethical Hacking	**Module Leader:** Paolo Modesti
	Module Code: Please refer to Cover page
Assignment Title: ICA (100%)	**Deadline Date:** Please refer to Cover page **Deadline Time: TBC**
	Submission Method: Online (Blackboard) ☑ Middlesbrough Tower ☐

Online Submission Notes:

- Please follow carefully the instructions given on the Assignment Specification
- When Extenuating Circumstances (e.g., extension) has been granted, a fully completed and signed Extenuating Circumstances form must be submitted to the School Reception or emailed to scedt-assessments@tees.ac.uk.

Central Assignments Office (Middlesbrough Tower M2.08) Notes:

- All work (including DVDs etc) needs to be secured in a plastic envelope or a folder and clearly marked with the student name, number and module title.
- An Assignment Front Sheet should be fully completed before the work is submitted.
- When Extenuating Circumstances (e.g. extension) has been granted, a fully completed and signed Extenuating Circumstances form must be submitted to the School Reception or emailed to scedt-assessments@tees.ac.uk.

FULL DETAILS OF THE ASSIGNMENT ARE ATTACHED INCLUDING MARKING & GRADING CRITERIA

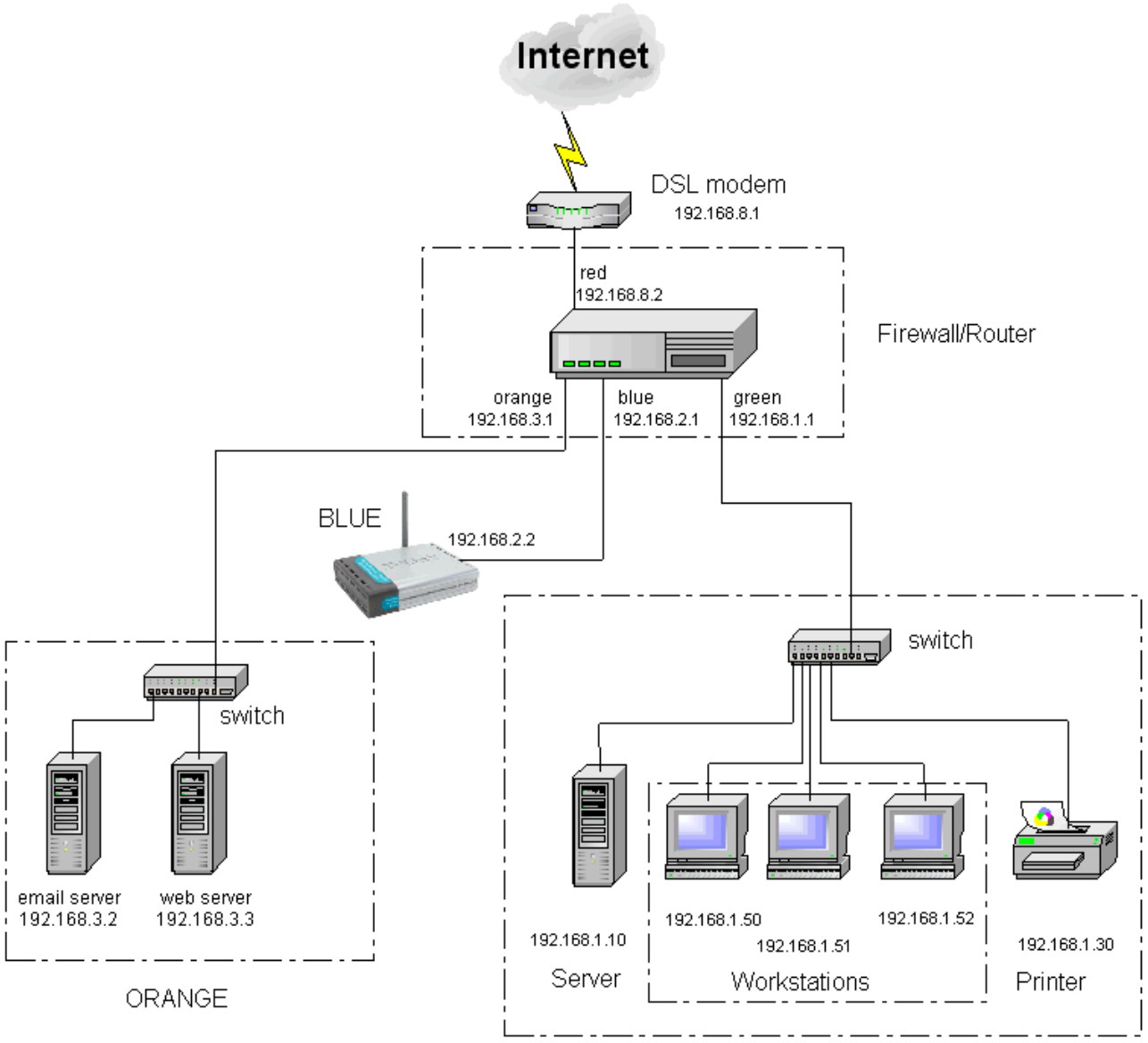
Scenario

A not-for-profit organisation working on human rights protection ask you to plan, execute and document an ethical hack against their systems to assess their security. Moreover, based on your findings, you are required to provide advice on how to improve the security of the system.

The organization periodically receives reports from whistle-blowers and independent advisors regarding alleged systematic violations of human rights in different countries. These reports could constitute support documentation for actions taken by the organisation such as legal action against alleged offenders or media campaigns.

The organisation is concerned that a possible data breaches that may compromise the confidentiality of the information and the identity of whistle-blowers and advisors.

For your security analysis, they provide you the following scheme and details:



A Linux based firewall/router controls the access to different zones of the system (zones are separate network entities, with no traffic across zones allowed without special permission):

Red — the Internet
Green — the safe zone for maximum protection
Orange — a DMZ designed for Web, mail, or other Internet servers
Blue — for wireless networks

Orange Zone:
The webserver is an Ubuntu 20.04 LTS machine running Apache 2.4.x
The email server is a MS Windows Server 2019 Standard, running MailEnable Standard Edition 10.41

Green Zone:
The Server: Windows Server 2019, with Active Directory, DHCP, DNS, IIS. The server also run a MySQL Server 8.0.30, the back end for a custom web application that is used by the admin and financial office. The server contains also shared folders, which are used for different purposes: projects, advisors reports, and other classified and non-classified documents
The workstations are Windows 10 21H2 machines.

Blue Zone:
Employees and volunteers are allowed to bring their own device and connect to the Internet.

No further information and no credentials are given except the public IP address and the domain name of the web server (since this information is purely hypothetical, we simply use these placeholders <PUBLIC_IP_ADDRESS> and <DOMAIN_NAME> to indicate them in your report).

Client requirements

The client specifically requests that:

- No data should be lost from any system during the pen testing. If any change is done, for a proof-of-concept, you should also identify a procedure to restore the system to the previous state, provided the pen-tester has double checked with client that a back up exists and it is safely stored.
- The risk of disrupting the services should be minimised during office hours.
- You have a limited number of hours for this task, so your planning should prioritise the key services and components.
- The pen testing activities should be carried out with FOSS or free software unless such option does not exist for a specific task. In this case, you should make clear the licence terms and costs.

Task

You should write a report (approximately 4500 words, submitted in PDF format) detailing your plan, with a justification for tools and techniques used, the results and a complete chronological audit trail of hacking actions taken in line with expected professional and ethical standards.

For the practical part, you must carry out a pen testing limited to a given virtual machine (information about location of the virtual machine is available on Blackboard, under "Assessment"). For the rest of the work, use the information provided in the scenario, and make the appropriate and reasonable assumptions if necessary (provide a rationale for it).

The report will have to cover all the stages of the ethical hacking methodology. The report should include at least the following elements (xx% indicates the weight in the mark allocation):

1. Demonstration of understanding of the scenario and discussion of the pre-engagement interactions. (10%)
2. Identification of relevant tools for each stage of the ethical hacking. (10%)
3. Appropriate information gathering and threat modelling (10%)
4. Identification of security vulnerabilities (10%)
5. Exploitation of the vulnerabilities (10%)
6. Post exploitation activities (10%)
7. Reporting of the findings and potential suggestions for countermeasures (10%)
8. Critical reflection of self-performance and the development of skills for employment as a computer security professional. (10%)

The remaining 20% of the final grade is allocated based on the overall quality of the report: formatting, completeness, readability, and appropriate referencing.

Elements 4, 5, 6, 7 are relevant for the practical part (as you must report the analysis of the given component) and the results of such activities should be documented and explained, also using appropriate screenshots.

For the element 7 you should also include countermeasures and recommendations deduced from the scenario, but they should be clearly separated from ones deduced from the practical elements.

N.B. The component provided for the practical part is not depicted in the diagram, but you can assume it is in the Orange zone and you have direct access to it.

Students will be assessed on the following learning outcomes:

1. Communicate effectively and professionally to report on system security.
2. Create and maintain an audit trail of all process undertaken during an ethical hack.
3. Apply tools and techniques in a structured, ethical, and professional manner to evaluate system security using ethical hacking methodologies.
4. Demonstrate knowledge of appropriate security analysis techniques, common vulnerabilities, and countermeasures.
5. Identify the professional, ethical, and legal issues associated with ethical hacking.
6. Operate ethically and within professional guidelines whilst conducting security testing.

Marking Criteria

Marks are provided as a guidance

A/A+/A++ 75%/85%/95%	*Excellent* An excellent answer demonstrating informed judgements about the task/scenario. Appropriate measures are selected and justified clearly. Autonomy of investigation is shown. Demonstrated excellent consideration of relevant professional, legal and ethical issues with very good linkage to the scenario/task. A very clear and readable report, with excellent structuring, good use of grammar and referencing. Document submitted as PDF. An excellent completion of the practical elements.

B 65%	*Substantially correct/appropriate (based on taught material & module requirements)* A good answer demonstrating informed judgements about the task/scenario. Appropriate measures are selected and justified. Autonomy of investigation is shown. Demonstrated appropriate consideration of relevant professional, legal and ethical issues in relation to the scenario/task. A clear and readable report, with appropriate structuring and referencing. Document submitted as PDF. A good completion of the practical elements.

C 55%	*Minor errors/omissions/issues* A mostly good answer with only minor errors/omissions/issues. The answer demonstrates informed judgements about the task/scenario. Appropriate measures are selected and justified. Some autonomy of investigation is shown. Demonstrated fairly appropriate consideration of relevant professional, legal and ethical issues in relation to the scenario/task with only minor errors/omissions/issues. A clear and readable report, with minor errors in writing, structure or referencing. Document submitted as PDF. A fairly good completion of the practical elements.

D 45%	*Major errors/omissions/issues* A limited answer with major errors/omissions/issues. The answer demonstrates some informed judgements about the task/scenario. Some appropriate measures are selected and justified. Limited autonomy of investigation is shown. Demonstrated some consideration of relevant professional, legal and ethical issues in relation to the scenario/task with major errors/omissions/issues. A report, with major issues of writing, structure or referencing. Document submitted as PDF. A sufficient completion of the practical elements

E 35%	*Unsatisfactory* A very limited answer. The answer demonstrates some few judgements about the task/scenario. Few measures are selected and justified. Little autonomy of investigation is shown. Little consideration of relevant professional, legal and ethical issues in relation to the scenario/task. A report that is difficult to read or comprehend but includes some attempt at structure and referencing *OR* document is not submitted as a PDF. An insufficient attempt to complete the practical part.
F 0%-20%	*Inadequate* The answer barely addresses the task/scenario, if at all. Little to no consideration of professional, legal, and ethical issues. A report that is very difficult to read and comprehend and makes no attempt at referencing. No or very limited attempt to complete the practical elements.